**Spam w lutym: możesz stać się częścią botnetu**

**Eksperci z Kaspersky Lab przeanalizowali ewolucję spamu w lutym 2014 r. Odnotowano wiele szkodliwych załączników przychodzących wraz ze spamem stanowiącym rzekomo wiadomości e-mail wysyłane przez kobiety, które przy okazji walentynek chciały poznać nowych przyjaciół.**

Niektórzy spamerzy posunęli się jeszcze dalej, próbując złapać odbiorców na obietnicę zdjęć zawartych w załączonym do wiadomości archiwum. Pojawiło się również więcej konwencjonalnych szkodliwych masowych wysyłek imitujących powiadomienia z popularnych portali społecznościowych, w tym z Facebooka.

Lutowy szkodliwy spam o tematyce miłosnej zdominowały trojany – za pomocą masowych wysyłek cyberprzestępcy infekowali łatwowiernych użytkowników szkodnikiem, który instaluje w systemie dwa niebezpieczne programy. Pierwszy to program szpiegowski (tzw. spyware), który kradnie z komputera wszystkie pliki z dokumentami docx, xlsx, oraz pdf i wysyła je na określoną skrzynkę pocztową. Drugi szkodnik to bot/robak IRC o nazwie ShitStorm, który przeprowadza ataki DDoS na strony internetowe i rozprzestrzenia swoje kopie za pośrednictwem usług MSN oraz P2P. Jeżeli odbiorcy odpowiedzą na tego rodzaju wiadomości e-mail, ich komputer może łatwo zostać przyłączony do botnetu, czyli sieci zainfekowanych maszyn kontrolowanej przez cyberprzestępców. Oprócz aplikacji szpiegowskiej lutowy szkodliwy spam zawierał również ransomware – rodzaj szkodliwego oprogramowania, które blokuje komputer użytkownika, a następnie żąda pieniędzy za udzielenie dostępu. Rzekome zdjęcia załączone do wiadomości również okazały się szkodliwymi programami. Jednym z nich był backdoor Andromeda, który pozwala cyberprzestępcom potajemnie kontrolować zainfekowany komputer.

Inny szkodliwy program podszywał się pod powiadomienia z najpopularniejszych portali społecznościowych. Były one rzekomo wysyłane przez zespół Facebooka i informowały odbiorcę, że od czasu jego ostatniej wizyty dużo się działo u jego znajomych, po czym zachęcały do otworzenia załączonego archiwum. Niestety zawierało ono backdoora ze wspomnianej wcześniej rodziny Andromeda.

**Luty w liczbach**

Udział spamu w ruchu pocztowym w lutym zwiększył się o 4,2 punktu procentowego w porównaniu z poprzednim miesiącem i wynosił średnio 69,9% - o 1,2 punktu procentowego mniej niż w lutym 2013 r.

Do czołówki rankingu największych źródeł spamu powróciły Chiny (23%), za którymi uplasowały się Stany Zjednoczone (19,1%) oraz Korea Południowa. Polska znalazła się na 15 miejscu z wynikiem 0,94%.

Wśród 3 organizacji najczęściej atakowanych przez phisherów znalazły się: portale społecznościowe (27,3%), serwisy e-mail (19,34%) oraz organizacje e-płatności (16,73%). W lutym specjaliści z Kaspersky Lab natrafili również na fałszywe powiadomienia, które podszywały się pod malezyjski bank HongLeong.

„Wiadomości phishingowe żerujące na nazwach znanych organizacji finansowych oraz e-płatności z różnych państw są aktywnie wysyłane przez oszustów, którzy chcą ukraść dane finansowe. Udany atak zwykle zapewnia phisherom pełny dostęp do prywatnego konta ofiary na stronie internetowej banku” – powiedziała **Tatjana Szczerbakowa**, starszy analityk spamu w Kaspersky Lab.

Pełny raport poświęcony ewolucji spamu w lutym 2014 r. pojawi się już wkrótce w serwisie [SecureList.pl](http://securelist.pl) prowadzonym przez Kaspersky Lab.

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky Lab jako źródła.

Wszystkie informacje prasowe Kaspersky Lab Polska są dostępne na stronie <http://www.kaspersky.pl/news>.